Mathematics 1214: Introduction to Group Theory

Solutions to homework exercise sheet 9

1. Let G and H be two groups. Prove that $G \times H$ is abelian if and only if G is abelian and H is abelian.
   [Hint: for " $\implies$ ", first think about elements of the form (g, e_H).]

   Solution " $\implies$ " Suppose that $G \times H$ is abelian. If $g_1, g_2 \in G$ then

   $$(g_1g_2, e_H) = (g_1, e_H)(g_2, e_H) \overset{G \times H \text{ abelian}}{=} (g_2, e_H)(g_1, e_H) = (g_2g_1, e_H),$$

   so $g_1g_2 = g_2g_1$. So G is abelian. Similarly, we have $(e_G, h_1h_2) = (e_G, h_1)(e_G, h_2) = (e_G, h_2)(e_G, h_1) = (e_G, h_2h_1)$ so $h_1h_2 = h_2h_1$ for all $h_1, h_2 \in H$, so H is abelian.

   "$\Longleftarrow$" Suppose that G and H are abelian. If $x_1, x_2 \in G \times H$ then $x_1 = (g_1, h_1)$ and $x_2 = (g_2, h_2)$ for some $g_1, g_2 \in G$ and $h_1, h_2 \in H$, so

   $$x_1x_2 = (g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) \overset{G, H \text{ both abelian}}{=} (g_2g_1, h_2h_1) = (g_2, h_2)(g_1, h_1) = x_2x_1.$$

   So $x_1, x_2 \in G \times H \implies x_1x_2 = x_2x_1$, so $G \times H$ is abelian.

2. Let p, q be prime integers. Show that if G is a group with $|G| = pq$ and $H \leq G$, then either $H = G$, or H is a cyclic subgroup of G.

   [Remark: in mathematics, the statement "A or B" means that one of the three possibilities "A and not B", "B and not A", "A and B" is true. In other words, "A or B" can be thought of as "A, or B, or both".]

   [Hint: if $k \in \mathbb{N}$ and p and q are primes with $k < pq$, then $k|pq \implies k|p$ or $k|q$.]

   Solution If $H \leq G$ then either:

   (a) $|H| = |G| \implies H = G$; or

   (b) $|H| < |G|$. In this case, Lagrange's theorem shows that $|H| \,\Big|\, |G| = pq$, so $|H| \,\Big|\, p$ or $|H| \,\Big|\, q$ by the hint. Since p and q are prime, this gives $|H| = 1$ or $|H| = p$ or $|H| = q$. So there are three cases:

      (i). $|H| = 1 \implies H = \{e\} = \langle e \rangle$, so H is cyclic; or

      (ii). $|H| = p$, so H is a (sub)group of prime order, so H is cyclic by Corollary 39; or

      (iii). $|H| = q$, so H is a (sub)group of prime order, so H is cyclic by Corollary 39 again.

      Hence if $|H| < |G|$ then H is a cyclic subgroup of G.

   In summary, we've shown that if $H \leq G$ then either $H = G$ or H is a cyclic subgroup of G.

3. Given the group G below, determine the number of (different) subgroups of G, and list them. Also determine whether or not G is a cyclic group.

   (a) $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ (b) $G = \mathbb{Z}_2 \times \mathbb{Z}_3$

Solution (a) We have $|G| = |\mathbb{Z}_2 \times \mathbb{Z}_2| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_2| = 2 \cdot 2$. Since 2 is prime, by Exercise 2, every subgroup other than G itself is cyclic. The cyclic subgroups are:

- $\langle e \rangle = \{e\}$ where $e = ([0], [0])$ is the identity element of G,
- $\langle ([0], [1]) \rangle = \{e, ([0], [1])\}$,
- $\langle ([1], [0]) \rangle = \{e, ([1], [0])\}$,
- $\langle ([1], [1]) \rangle = \{e, ([1], [1])\}$,

and the only other subgroup is G itself. So there are five subgroups. Since $\langle a \rangle \neq G$ for all $a \in G$, the group G is not cyclic.

(b) We have $|G| = 2 \cdot 3$, and 2 and 3 are prime, so by Exercise 2 every subgroup other than G itself is cyclic. These cyclic subgroups are:

- $\langle e \rangle = \{e\}$ where $e = ([0], [0])$ is the identity element of G,
- $\langle ([0], [2]) \rangle = \langle ([0], [1]) \rangle = \{e, ([0], [1]), ([0], [2])\}$
  [the first equality is a special case of $\langle a^{-1} \rangle = \langle a \rangle$, since $([0], [1])^{-1} = ([0], [2])$],
- $\langle ([1], [2]) \rangle = \langle ([1], [1]) \rangle = \{e, ([1], [1]), ([0], [2]), ([1], [0]), \dots\} = G$ (since this calculation shows that this set contains at least 4 elements and its order must divide 6, so it must contain all 6 elements)
- $\langle ([1], [0]) \rangle = \{e, ([1], [0])\}$.

So there are four subgroups. Since $G = \langle ([1], [1]) \rangle$, G is cyclic.

4. Let $n \geq 2$ be a non-prime integer, and suppose that G is a cyclic group of order n with identity element e. Prove that there is a subgroup of G other than $\{e\}$ and G. [This is a partial converse to Corollary 39].

Solution We have $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ for some $a \in G$, and $o(a) = n$. Since n is not prime and $n \geq 2$, there are integers s, t with $1 < s, t < n$ and $st = n$. Let $b = a^s$ and let $H = \langle b \rangle$. Then H is a subgroup of G with $|H| = o(b) > 1$, so $H \neq \{e\}$. Also, $b^t = (a^s)^t = a^{st} = a^{o(a)} = e$, so $o(b) \leq t < n$, so $|H| < |G|$, so $H \neq G$.

5. Let $n \geq 3$ and write $D_n = \{\iota, \rho, \rho^2, \rho^3, \dots, \rho^{n-1}, r_0, r_1, r_2, \dots, r_{n-1}\}$ where, as usual, ι is the identity element of D_n, r_j is reflection in the line through the origin making an angle of π/n with the positive x-axis, and ρ is rotation by $2\pi/n$ counterclockwise.

   Consider the following subgroups of D_n:

$$\langle \iota \rangle,\ \langle r_0 \rangle,\ \langle r_1 \rangle,\ \dots,\ \langle r_{n-1} \rangle,\ \langle \rho \rangle,\ D_n.$$

   (a) Compute the order of each of these subgroups, and prove that no two of these subgroups are equal.

   (b) Prove that if n is prime then there are no other subgroups of D_n.
   [Hint: use Exercise 2]

   (c) Prove that if n is not prime, then there is a subgroup of D_n that is not in this list.

Solution (a) We have $|\langle\iota\rangle| = o(\iota) = 1$, $|\langle r_j\rangle| = o(r_j) = 2$ and $|\langle\rho\rangle| = o(\rho) = n$ and $|D_n| = 2n$. So

- $\langle\iota\rangle$ is the only subgroup in the list of order 1
- $\langle\rho\rangle$ is the only subgroup in the list of order n, and
- D_n is the only subgroup in the list of order $2n$.

So none of these is equal to any of the others.

Now $\langle r_i\rangle = \{\iota, r_i\}$, so if $\langle r_i\rangle = \langle r_j\rangle$ then $\{\iota, r_i\} = \{\iota, r_j\}$, so $r_i = r_j$. So the n subgroups $\langle r_k\rangle$ for $0 \le k < n$ are all different.

(b) If n is prime then $|D_n| = 2n$ is the product of two primes, so by Exercise 2, every subgroup other than D_n is cyclic. The cyclic subgroups of D_n are the subgroups $\langle a\rangle$ for some $a \in D_n$.

We need to show that these are all listed above.

It looks like we're missing the cyclic subgroups $\langle b\rangle$ where $b = \rho^k$ for $1 < k < n$, but we'll show that these are all equal to $\langle\rho\rangle$.

In fact, $\langle\rho\rangle$ is a group of prime order, so by Corollary 39(b), $\langle\rho\rangle = \langle b\rangle$ for any $b \in \langle\rho\rangle$.

So the list does indeed contain all of the cyclic subgroups as well as D_n, so it contains all the subgroups of D_n.

(c) Suppose n is not prime. If $n = 4$ then $H = \{\iota, \rho^2, r_0, r_2\}$ is a subgroup of D_4 of order 4. Since every element of H has order 1 or 2, the subgroup H is not cyclic (otherwise, it would contain an element of order 4) and $H \neq D_4$ since D_4 contains 8 elements and H only contains 4 elements. So H is not in the list above.

If $n > 4$ then, since n is not prime, it has a proper divisor (that is, a divisor apart from 1 and n) which is larger than 2. Hence $n = st$ for some integers s, t with $1 < s < n$ and $2 < t < n$. Now $(\rho^s)^k = \rho^{sk}$, so $o(\rho^s)$ (the smallest positive integer k such that $(\rho^s)^k = \iota$) is t. Hence $2 < |\langle\rho^s\rangle| = t < n$, so this is a subgroup of D_n which is not in the list above.

OR: if $n > 4$ then write $n = st$ where $2 < t < n$ and observe that $D_t \le D_n$ and $|D_t| = 2t < 2n = |D_n|$, so $D_t \neq D_n$, and since D_t is non-abelian, it is not cyclic so it's not in the list above.